Simplifiez la gestion de vos certificats SSL dans toute l'entreprise

Simplifiez la gestion de vos certificats SSL dans toute l'entreprise

Introduction

L'utilisation de certificats SSL dépasse désormais le simple cadre des pages d'achat pour s'étendre aux fonctions vitales de l'entreprise. Ce faisant, ils permettent de protéger l'ensemble des communications électroniques, à savoir les e-mails, chats et messages instantanés des collaborateurs distants et autres partenaires de l'entreprise. De même, sur le Cloud, les échanges navigateur-serveur exigent le déploiement de certificats SSL dès lors qu'ils impliquent l'affichage de données comptes-clients, de transactions entre partenaires et d'outils de productivité des utilisateurs. Enfin, les certificats SSL sécurisent les communications serveur-serveur dans le cadre d'applications et d'échanges de données.

Cependant, la gestion d'un parc de certificats SSL présente un certain nombre de défis, notamment dans les multinationales et autres grands groupes très actifs dans le développement de services Web. Or, l'expiration d'un certificat SSL peut avoir des répercussions multiples : manque à gagner, érosion de la confiance des clients, réduction des capacités d'action des collaborateurs et partenaires, et vulnérabilité des données confidentielles. Face à ces scénarios catastrophe, la gestion efficace de certificats SSL dispersés dans les méandres de réseaux complexes revêt une importance capitale pour l'entreprise. L'enjeu : assurer une protection continue par la prévention de toute expiration intempestive de certificats.

Ce guide a pour objectif de vous accompagner à travers les cinq étapes charnières d'une maîtrise totale de votre parc de certificats SSL. Les informaticiens y trouveront également des conseils précieux pour la mise en place d'une console de gestion centralisée, gage d'une visibilité totale tout au long du cycle de vie des certificats.

Les cinq étapes d'une maîtrise totale de votre parc de certificats SSL et Code Signing

Le contrôle de l'ensemble des certificats SSL de votre entreprise passe par ces cinq étapes charnières :

1. Effectuez un audit de tous vos domaines et certificats.
2. Consolidez tous vos certificats au sein d'un compte géré et centralisé.
3. Définissez un processus administratif applicable à toute l'entreprise.
4. Programmez des alertes et produisez des rapports réguliers sur la situation du parc et les renouvellements imminents.
5. Révoquez et remplacez les certificats en cas de besoin.

1. Effectuez un audit de tous vos domaines et certificats.

Êtes-vous réellement en mesure de localiser tous vos certificats SSL, sans exception ? Ne vous y trompez pas : seule une visibilité totale de tous les certificats Thawte SSL déployés dans votre entreprise vous permettra de sécuriser véritablement les transactions en ligne, communications et autres applications Web. En ce sens, pour la constitution d'un inventaire comme pour la validation d'une liste existante, un outil de découverte des certificats vous aidera à automatiser le processus de détection et le catalogage d'informations essentielles : localisation exacte du certificat SSL ou Code Signing, date d'expiration, période de validité et longueur de la clé.

Résultat : un reporting en temps réel de tous les certificats présents sur des domaines sécurisés.

SCÉNARIO : L'EXPIRATION MYSTÈRE

Un serveur e-commerce s'arrête soudainement, sans que personne ne sache vraiment pourquoi. Et pendant que l'équipe informatique s'échine à trouver la panne, l'horloge tourne et le manque à gagner se chiffre en milliers de ventes par heure. Finalement, le mystère est enfin percé. En cause : l'expiration d'un certificat acheté auprès d'une autorité non validée, par un collaborateur qui a depuis quitté l'entreprise. Par conséquent, l'avis de renouvellement n'est jamais parvenu à l'administrateur actuel, sans que personne ne connaisse d'ailleurs la présence de ce certificat « fantôme » sur le réseau. Pour éviter ce type d'incident, le compte Thawte Certificate Center Enterprise permet aux administrateurs de visualiser tous les certificats Thawte au sein du réseau de l'entreprise.

2. Consolidez tous vos certificats au sein d'un compte géré et centralisé.

L'audit vous livre toutes les informations nécessaires à l'évaluation de votre protection SSL et à la consolidation des certificats au sein d'un compte géré et centralisé, synonyme de resserrement de votre contrôle. À la lecture de l'audit, assurez-vous de vous poser les bonnes questions :

- Les certificats sont-ils tous correctement installés ?
- Les certificats sont-ils dotés des niveaux de cryptage et d'authentification adaptés ?
- Les marques de confiance et sceaux de sécurité apparaissent-ils sur les pages clés ?
- Tous les serveurs à protéger sont-ils équipés d'un dispositif de sécurité SSL ?
- Existe-t-il des certificats non-autorisés à ramener dans le champ de contrôle ?

Les certificats SSL actuels offrent différents niveaux de cryptage et d'authentification. Pour gérer ce parc hétérogène, les outils de gestion classiques imposent des identifiants de connexion propres à chaque type de certificat. Or, à mesure que l'entreprise se développe et que les administrateurs IT se multiplient, difficile de coordonner une telle quantité de comptes sans un point de contrôle central. Il existe cependant une solution : à mesure que les dates d'expiration approchent, pensez à remplacer les certificats en question par les certificats d'un compte géré offrant toute la palette d'options SSL. Ce faisant, vous bénéficierez également de remises sur volumes, avec à la clé une baisse des coûts.

Résultat : un compte centralisé pour la gestion de tous les certificats de l'entreprise.

SCÉNARIO : LE PROJET DE CONSOLIDATION

Une récente fusion d'entreprise impose l'intégration de deux réseaux, à commencer par l'achat de cinq certificats SSL premium et cinq certificats standard, sans oublier l'actualisation des coordonnées sur trois certificats existants. Or, l'achat de nouveaux certificats risque de détourner vos ressources d'autres activités d'intégration critiques. Grâce au compte Thawte Certificate Center Enterprise, vous effectuez instantanément l'achat et le renouvellement groupés de plusieurs certificats à la fois.

Compte Thawte Certificate Center Enterprise

Points forts	Avantages
Portail de gestion sur le Web	L'interface ultra-fonctionnelle facilite la configuration et le déploiement de certificats, pour une gestion complète du cycle de vie.
Contrôle centralisé	Consolidation de l'achat et de la gestion des certificats sur l'ensemble des sites et divisions, avec à la clé une réduction sensible des coûts.
Customisation des workflows et pistes d'audit	Délégation des tâches administratives et prévalidation de domaines pour une émission instantanée de certificats à la demande, avec en prime une piste d'audit intégrale pour une traçabilité totale des opérations.
Gamme complète de certificats SSL	Gestion de tous les types de certificats sur une seule et même console : Extended Validation (EV), SGC, SAN pour communications unifiées, SSL standard et Code Signing.
Reporting fiable	Accès basé sur les rôles à différents types de rapports (temps réel, hors ligne, mensuels) pour mieux gérer les ressources et les risques.
Alertes et notifications customisables	Alertes envoyées automatiquement à de multiples destinataires pour éviter toute perte de communication.
Support irréprochable	Assistance téléphonique, par e-mail et sur le Net.

3. Définissez un processus administratif applicable à toute l'entreprise.

Un compte de gestion centralisée permet aux administrateurs autorisés d'effectuer des achats groupés de certificats à répartir sur toute la structure de l'entreprise. L'administrateur définit lui-même le processus de gestion en fonction du niveau de contrôle souhaité : qui dispose de quels privilèges, quelle est la procédure de délégation et qui reçoit quel type de notifications.

Ce système de gestion doit être assez flexible et modulable pour s'adapter à votre environnement. Les accès basés sur les rôles et autres octrois dynamiques de privilèges permettent d'appliquer les processus administratifs définis. Ainsi, lorsque les administrateurs se connectent au moyen de leurs identifiants personnels, ils ont la possibilité de gérer leurs certificats en fonction de leurs rôles et de la division à laquelle ils sont rattachés.

De même, lorsqu'un administrateur soumet une demande de certificat SSL ou Code Signing, cette requête peut donner lieu à une émission instantanée, un refus ou une mise en attente, selon un ensemble de règles préétablies.

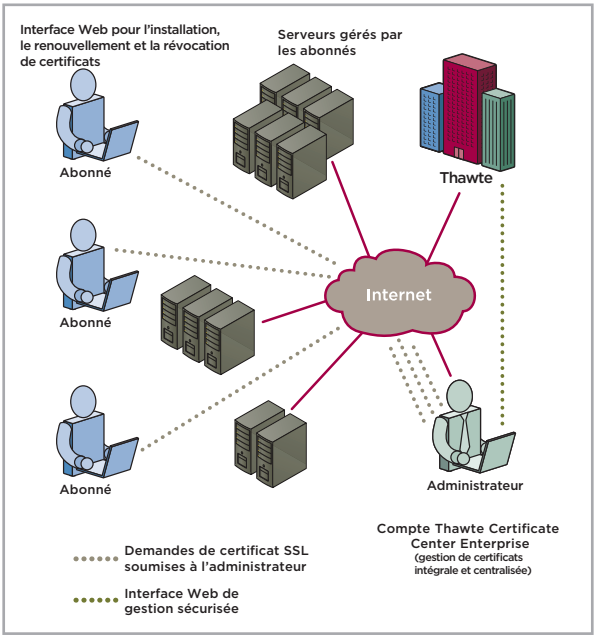
Pour la plupart des certificats SSL, l'acheteur devra fournir les coordonnées d'un interlocuteur technique (nom, téléphone et e-mail). Le format des coordonnées, tout comme le paramétrage des notifications, devront être en phase avec le processus administratif en place. Quant aux préavis d'expiration, ils pourront être envoyés par e-mail à plusieurs administrateurs, voire à un alias de type adminssl@votredomaine.com. Dans une même optique, la programmation des notifications permettra de rationaliser le processus tout en tenant les administrateurs informés. Quelques exemples :

- Lorsque le nombre de certificats en production descend en deçà d'un certain seuil, l'administrateur reçoit un message l'avertissant du besoin d'achat de nouveaux certificats.
- Des alertes incitent les administrateurs à se connecter à la plate-forme pour étudier les demandes en cours.
- Des e-mails de confirmation informent les administrateurs en cas d'émission instantanée d'un certificat.

Résultat : un processus administratif clairement défini et intégré au système de gestion.

SCÉNARIO : CONTRÔLE LOCAL, SUPERVISION CENTRALE

Basée en Inde, votre équipe de programmeurs souhaite installer un certificat sur un serveur de développement local. Seul problème : le décalage horaire entraîne un délai de 24h entre la demande et votre feu vert. Un retard coûteux et évitable dans la mesure où il s'agit d'un certificat pré-approuvé, demandé par un utilisateur authentifié sur un domaine autorisé. La solution : se connecter au compte Thawte Certificate Center Enterprise pour déléguer les droits administratifs et permettre une émission instantanée des certificats à l'avenir.



Types d'utilisateurs	Avantages
Administrateur principal du compte	Définit les rôles, les privilèges et les accès aux assistants dont bénéficient les autres administrateurs.
Administrateur délégué ou départemental	Responsable de la gestion des certificats pour un domaine, un département ou une division donnée ; autorise ou refuse les demandes de certificats, révoque les certificats et redirige certaines requêtes vers d'autres administrateurs.
Accès en lecture seule	Consultation de divers types de rapports : requêtes en cours, données relatives aux certificats et fichiers journaux.

4. Programmez des alertes et produisez des rapports réguliers sur la situation du parc et les renouvellements imminents.

La plate-forme de gestion des certificats produit des rapports réguliers permettant aux administrateurs systèmes de mieux gérer leur temps et leurs ressources. Ainsi, ils ont la possibilité de lancer des rapports instantanés sur la situation détaillée de chaque certificat du parc : demandes d'émission et certificats opérationnels, en attente, approuvés, refusés, valides, révoqués, désactivés, expirés ou sur le point d'expirer. Quant aux alertes de renouvellement avec préavis de 30, 60 ou 90 jours, elles aident les administrateurs à mieux planifier leurs réabonnements pour profiter de remises sur volumes. Enfin, l'analyse des historiques leur permet de bien cerner les usages passés pour mieux planifier et gérer leurs certificats à terme.

La customisation et la prise en charge de multiples formats permettent une intégration maximale aux processus et outils administratifs existants. L'administrateur doit avoir la possibilité de personnaliser les rapports détaillés d'utilisation des certificats par entité ou administrateur, sans oublier l'automatisation du reporting en vue d'une diffusion régulière aux contacts clés. Enfin, la prise en charge de divers formats (PDF, HTML et CSV) facilite le partage et l'intégration des informations pour leur consultation et analyse ultérieures.

Résultat : allocation des ressources et définition du budget SSL sur une base annuelle.

5. Révoquez et remplacez les certificats en cas de besoin.

Dans le prolongement d'une consolidation des certificats, les outils de gestion facilitent leur révocation et leur remplacement. Lorsque des serveurs sont mis hors ligne, déplacés ou remplacés, les certificats SSL doivent suivre le même processus à l'aide des fonctions « révoquer » ou « remplacer ». De même, en cas de perte ou de compromission d'une clé ou de défaillance d'un serveur entraînant la suppression d'un certificat, l'administrateur devra révoquer les certificats concernés et installer des certificats de remplacement. Pour ce faire, les clients Thawte Enterprise bénéficient d'un service gratuit de révocation et de remplacement des certificats. Ils peuvent ainsi réaffecter des certificats sans perdre de temps.

Résultat : davantage de contrôle sur les certificats perdus ou disparus.

SCÉNARIO : LA RELOCALISATION

La fusion de deux datacenters vous oblige à déplacer des certificats d'un site physique vers un autre. Pour vous, pas question d'acheter de nouveaux certificats et de perdre au passage la période de validité restante sur les certificats existants. Pour autant, vous ne pouvez pas non plus vous permettre une quelconque interruption de la protection. La fonctionnalité « révoquer et remplacer » du compte Thawte Certificate Center Enterprise vous permet de déplacer facilement les certificats d'un site physique à un autre.

Un point de contrôle centralisé pour une visibilité totale

À défaut d'outils appropriés, la gestion manuelle d'un parc étendu de certificats, à travers des infrastructures complexes, s'avère à la fois chronophage et source d'erreurs. Certes, la mise en place d'une autorité de certification (AC) interne, capable d'autosigner des certificats, offre le point de contrôle centralisé que vous recherchez. Mais outre l'investissement initial conséquent, le développement d'une telle infrastructure prend énormément de temps, sans compter qu'elle doit faire l'objet d'évolutions constantes pour la prise en charge de nouveaux types de certificats, notamment SSL EV (Extended Validation).

Le compte Thawte Certificate Center Enterprise associe les fonctionnalités leaders d'une AC de confiance aux avantages pratiques de l'autosignature : point de contrôle centralisé sur une infrastructure ultra fiable et évolutive, fonction de découverte de tous les certificats Thawte SSL et Code Signing présents dans l'entreprise, etc. Côté gestion, une fois les certificats achetés et le compte client créé, les administrateurs disposent de toute la latitude nécessaire à la customisation du compte et à la délégation des responsabilités – sans les délais ni les coûts de configuration de l'infrastructure généralement associés.

- Déployé en mode SaaS, le compte Thawte Certificate Center Enterprise n'exige aucun investissement capital initial et offre un TCO particulièrement bas. Quant à l'infrastructure ultra fiable de Thawte, elle saura évoluer au rythme de votre croissance.
- L'association entre centralisation du contrôle et délégation flexible des responsabilités permet d'aligner la gestion de votre parc de certificats sur les workflows de votre entreprise. Dès lors qu'ils bénéficient des autorisations nécessaires, les administrateurs de domaines préapprouvés ont la possibilité d'émettre des certificats SSL sur de multiples serveurs, à la demande, tout en bloquant les achats de certificats sortant du cadre des procédures établies.

Principaux avantages :

BAISSE DU TCO

Contrôle centralisé, découverte de certificats, remises sur volumes… tous ces avantages contribuent à la réduction des coûts et de la complexité d'une gestion de multiples certificats SSL dans toute l'entreprise.

OPTIONS DE GESTION FLEXIBLES

De la délégation de responsabilités administratives à l'affectation dynamique de privilèges, en passant par les accès basés sur les rôles, vous établissez des niveaux de contrôle adaptés pour la gestion du cycle de vie intégral de tous les certificats.

- La gamme de certificats Thawte SSL propose différents niveaux de cryptage, d'authentification et de validité pour satisfaire les besoins spécifiques des entreprises, avec en prime le sceau Thawte Trusted Site.
- Le renforcement du contrôle et l'amélioration de la visibilité permettent de prévenir toute expiration intempestive et d'identifier les certificats non autorisés, avec à la clé une réduction des risques d'interruption des opérations et communications.

Conclusion

La gestion d'un parc de certificats SSL est devenue une opération complexe. Pour y faire face, le compte Thawte Certificate Center Enterprise offre une plate-forme à la fois simple, puissante et économique pour la découverte et la gestion de vos certificats. Fournie en mode SaaS, cette console permet aux administrateurs IT d'automatiser les tâches critiques, tout en réduisant les coûts et en atténuant les risques liés à la gestion des certificats de toute l'entreprise.

Pour en savoir plus, contactez nos conseillers commerciaux :

- **Par téléphone**
  - **États-Unis : +1 888 484 2983**
  - **Royaume-Uni : +44 203 450 5486**
  - **Afrique du Sud : +27 21 819 2802**
  - **Allemagne : +49 69 3807 89081**
  - **France : +33 1 57 32 42 68**
- **Par e-mail : Enterprisesales@thawte.com**
- **Sur notre site Web : http://www.thawte.fr/ssl/volume-discount-ssl-certificates/index.html**

Protégez votre activité et inspirez confiance à vos clients grâce à la sécurité renforcée des certificats numériques signés Thawte, leader mondial de la sécurité en ligne. Stabilité, fiabilité, infrastructure éprouvée, support client irréprochable… en 17 ans, Thawte a su s'imposer comme le partenaire international de choix pour les entreprises du monde entier.

UID 192/2/13